DOCKET NO.: 259551US6PCT/phh

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF:
Hideyuki SUZUKI

SERIAL NO: 10/509,872 GROUP: 2131

FILED: February 3, 2005 EXAMINER:

FOR: BROADCAST ENCRYPTION KEY DISTRIBUTION SYSTEM

LETTER

Mail Stop DD
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith is an International Written Opinion for the Examiner's consideration. The reference(s) cited therein have been previously filed on October 1, 2004.

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Raymond F. Cardillo Jr.

Bradley D. Lytle
Registration No. 40,073
Raymond F. Cardillo, Jr.
Registration No. 40,440

Customer Number
22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 10/05)

PATENT COOPERATION TREATY

Translation

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	18-05-2004
Applicant's or agent's file reference: JSONY-511PCT	FOR FURTHER ACTION: See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/JP2004/001076	03-02-2004	03-02-2003

International Patent Classification (IPC) or both national classification and IPC

H04L 9/08

Applicant

SONY CORPORATION

1. This opinion contains indications relating to the following items:

- ☒ Box No. I — Basis of the opinion
- ☐ Box No. II — Priority
- ☐ Box No. III — Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☒ Box No. IV — Lack of unity of invention
- ☒ Box No. V — Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI — Certain documents cited
- ☐ Box No. VII — Certain defects in the international application
- ☒ Box No. VIII — Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/JP	Date of completion of this opinion	Authorized officer
Facsimile No.		Telephone No.

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/JP2004/001076

Box No. I **Basis of the report**

1. With regard to the **language**, this opinion has been established on the basis of:

   ☐ the international application in the language in which it was filed

   ☐ the translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rule 12.3(a) and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material

      ☐ a sequence listing

      ☐ table(s) related to the sequence listing

   b. format of material

      ☐ on paper

      ☐ in electronic form

   c. time of filing/furnishing

      ☐ contained in the international application as filed

      ☐ filed together with the international application in electronic form

      ☐ furnished subsequently to this Authority for the purposes of search

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/JP2004/001076

Box No. IV Lack of unity of invention

1. ☐ In response to the invitation (Form PCT/ISA/206) to pay additional fees the applicant has, within the applicable time limit:

   ☐ paid additional fees

   ☐ paid additional fees under protest and, where applicable, the protest fee

   ☐ paid additional fees under protest but the applicable protest fee was not paid

   ☐ not paid additional fees

2. ☒ This Authority found that the requirement of unity of invention is not complied with and chose not to invite the applicant to pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rules 13.1, 13.2 and 13.3 is:

   ☐ complied with

   ☒ not complied with for the following reasons:

The inventions set forth in claims 1-6, 10-12, 15, 16 relate to broadcast key distribution for encrypting a payload or broadcast encryption key and a terminal identifier using a broadcast encryption key and transmitting them to another terminal.

The inventions set forth in claims 7-9, 13, 17 relate to unicast key distribution for encrypting and decrypting a broadcast key and a terminal identifier using a unicast encryption key.

The inventions set forth in claims 14 and 18 relate to key distribution via re-encryption processing, wherein the broadcast encryption key and the terminal identifier, which have been encrypted by the first terminal using the unicast encryption key, are decrypted by the second terminal, re-encrypted using the broadcast encryption key, and transmitted to a third terminal.

4. Consequently, this opinion has been established in respect of the following parts of the international application:

   ☒ all parts

   ☐ the parts relating to claims Nos. _____

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No. PCT/JP2004/001076

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	14, 18	YES
	Claims	1-13, 15-17	NO
Inventive step (IS)	Claims		YES
	Claims	1-18	NO
Industrial applicability (IA)	Claims	1-18	YES
	Claims		NO

2. Citations and explanations:

Document 1: JP 2001-136159 A (Sony Corp.), 18 May 2001 Filed 10-1-04

Document 2: JP 10-107832 A (Hitachi Software Engineering Co., Ltd.), 24 April 1998 Filed 10-1-04

The inventions set forth in claims 1-6, 10-12, 15 and 16 are disclosed in document 1 (entire text and figures 1-6) cited in the international search report and, therefore, lack novelty and do not involve an inventive step.

The inventions set forth in claims 7-9, 13 and 17 are disclosed in document 2 (in particular, paragraphs [0026]-[0028] and [0044]-[0058]; fig. 1-4) cited in the international search report and, therefore, lack novelty and do not involve an inventive step.

The inventions set forth in claims 14 and 18 do not involve an inventive step in the light of documents 1 and 2.

It would be easy for a person skilled in the art to apply the device set forth in document 1 which is capable of performing unicast or broadcast using a key table

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

corresponding to a MAC address to the system for distributing information among a plurality of terminals, which is set forth in document 2, wherein encryption and decryption between the first terminal and the second terminal is performed using a common key shared by the first terminal and a second terminal, and re-encryption is performed by the second terminal.

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/JP2004/001076

Box No. VIII **Certain observations on the international application**

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

Claims 1-3 are not fully supported by the description.

That is to say, only the fact that a unicast key is used is disclosed with reference to the feature of payload encryption and decryption of the broadcast frame between terminal A, which corresponds to the first terminal, and terminal B, which corresponds to the second terminal.